On mutually unbiased bases: Passing from d to d^2

Maurice Robert Kibler

On mutually unbiased bases: Passing from d to d^2 dimensions

M. R. Kibler[1,2,3]

[1]Université de Lyon, 37 rue du repos, 69361 Lyon, France

[2]Université Claude Bernard Lyon 1, 43 Bd du 11 Novembre 1918, 69622 Villeurbanne, France

[3]CNRS/IN2P3, Institut de Physique Nucléaire, 4 rue Enrico Fermi, 69622 Villeurbanne, France

E-mail : m.kibler@ipnl.in2p3.fr

Abstract

We show how to transform the problem of finding $d+1$ mutually unbiased bases in $\mathbb{C}^d$ into the one of finding $d(d+1)$ vectors in $\mathbb{C}^{d^2}$. The transformation formulas admit a solution when d is a prime number.

Keywords: finite–dimensional quantum mechanics; mutually unbiased bases; projection operators; Gauss sums

PACS: 03.65.Fd, 03.65.Ta, 03.65.Ud

1 Introduction

The determination of mutually unbiased bases (MUBs) is of pivotal importance in the theory of information and in finite quantum mechanics. Let us recall that two orthonormal bases of a unitary space are said to be unbiased if the modulus of the inner product of any vector of one basis with any vector of the other is independent of the considered vectors (see Section II for a definition of MUBs in $\mathbb{C}^d$). Such bases are useful in classical information (network communication protocols) [1] and quantum information (quantum state tomography and quantum cryptography) [2] as well as for the construction of discrete Wigner functions [3], the solution of the mean King problem [4] and the understanding of the Feynman path integral formalism [5]. They are at the root of a formulation of the Bohr complementarity principle for finite quantum systems.

There exist numerous ways of constructing sets of MUBs. Most of them are based on discrete Fourier transform over Galois fields and Galois rings, quadratic discrete Fourier transform of qudits, discrete Wigner distribution, generalized Pauli operators, generalized Hadamard matrices, mutually orthogonal Latin squares, finite geometry methods, angular momentum theory, Lie-like approaches, and phase states associated with a generalized Weyl-Heisenberg algebra (see [6] and [7] for a review on the subject).

The aim of this note is to introduce a transformation that makes possible to replace the search of $d+1$ MUBs in $\mathbb{C}^d$ by the determination of $d(d+1)$ vectors in $\mathbb{C}^{d^2}$.

2 Mutually unbiased bases in $\mathbb{C}^d$

Two distinct orthonormal bases

$$B_a = \{|a\alpha\rangle : \alpha = 0, 1, \ldots, d-1\} \tag{1}$$

and

$$B_b = \{|b\beta\rangle : \beta = 0, 1, \ldots, d-1\} \tag{2}$$

(with $a \neq b$) of the d-dimensional Hilbert space $\mathbb{C}^d$ ($d \geq 2$) are said to be unbiased if

$$|\langle a\alpha|b\beta\rangle| = \frac{1}{\sqrt{d}}, \tag{3}$$

where $\langle \, | \, \rangle$ denotes the inner product in $\mathbb{C}^d$. It is well-known that the maximum number of MUBs in $\mathbb{C}^d$ is $d+1$ and that a complete set of $d+1$ MUBs exists if d is prime or the power of a prime number [1], [8], [9]. On the other hand, it is not known if it is possible to construct a complete set of $d+1$ MUBs in $\mathbb{C}^d$ in the case where d is not the nth power ($n \in \mathbb{N}^*$) of a prime. However, in this case there exists at least 3 MUBs, a well-known result for $d = 6$. In spite of a great number of numerical studies, no more than 3 MUBs were obtained for $d = 6$ [10], [11], [12], [13], [14], in agreement with the fact that it is widely believed that only 3 MUBs exist for $d = 6$.

If we include the $a = b$ case, Eq. (3) leads to

$$|\langle a\alpha|b\beta\rangle| = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{\sqrt{d}}(1-\delta_{a,b}) \tag{4}$$

or equivalently

$$|\langle a\alpha|b\beta\rangle|^2 = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b}). \tag{5}$$

We note the presence of a modulus in Eqs. (4) and (5). This modulus certainly constitutes a handicap when performing numerical calculations.

3 Passing from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$

The problem of finding a complete set of $d+1$ MUBs in $\mathbb{C}^d$ amounts to find $d(d+1)$ vectors $|a\alpha\rangle$ satisfying Eq. (5), where $a = 0, 1, \ldots, d$ and $\alpha = 0, 1, \ldots, d-1$ (the indexes of type a refer to the bases and, for fixed a, the index α refers to one of the d vectors of the basis corresponding to a). By following the approach developed in [15] for positive operator valued measures and MUBs, we can transform this problem into a (possibly) simpler one (not involving a square modulus like in Eq. (5)). The idea of the transformation is to introduce a projection operator associated with the $|a\alpha\rangle$ vector.

Let us suppose that it is possible to find $d+1$ sets B_a (with $a = 0, 1, \ldots, d$) of vectors of $\mathbb{C}^d$ such that Eq. (5) is satisfied. It is thus possible to construct $d(d+1)$ projection operators

$$\Pi_{a\alpha} = |a\alpha\rangle\langle a\alpha|, \quad a = 0, 1, \ldots, d, \quad \alpha = 0, 1, \ldots, d-1. \tag{6}$$

From Eqs. (5) and (6), it is clear that the $\Pi_{a\alpha}$ operators (of rank-1) satisfy the trace conditions

$$\mathrm{Tr}\,(\Pi_{a\alpha}) = 1, \quad \mathrm{Tr}\,(\Pi_{a\alpha}\Pi_{b\beta}) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b}), \tag{7}$$

where the traces are taken over $\mathbb{C}^d$. Each operator $\Pi_{a\alpha}$ can be developed on an orthonormal basis $\{E_{pq} : p, q = 0, 1, \ldots, d-1\}$ of the space of linear operators on $\mathbb{C}^d$ (orthonormal with respect to the Hilbert-Schmidt inner product). In other words

$$\Pi_{a\alpha} = \sum_{p=0}^{d-1}\sum_{q=0}^{d-1} w_{pq}(a\alpha)E_{pq}. \tag{8}$$

The E_{pq} operators are generators of the $\mathrm{GL}(d, \mathbb{C})$ complex Lie group. Their main properties are

$$E_{pq}^\dagger = E_{qp},\ E_{pq}E_{rs} = \delta_{q,r}E_{ps},\ \mathrm{Tr}\,(E_{pq}) = \delta_{p,q},\ \mathrm{Tr}\left(E_{pq}^\dagger E_{rs}\right) = \delta_{p,r}\delta_{q,s},\ p, q, r, s \in \mathbb{Z}/d\mathbb{Z} \tag{9}$$

and they can be represented by the projectors

$$E_{pq} = |p\rangle\langle q|, \quad p, q \in \mathbb{Z}/d\mathbb{Z}. \tag{10}$$

The $w_{pq}(a\alpha)$ expansion coefficients in Eq. (8) are complex numbers such that

$$\overline{w_{pq}(a\alpha)} = w_{qp}(a\alpha), \quad p, q \in \mathbb{Z}/d\mathbb{Z}, \tag{11}$$

where the bar denotes complex conjugation.

By combining Eqs. (7) and (8), we get

$$\sum_{p=0}^{d-1}\sum_{q=0}^{d-1} \overline{w_{pq}(a\alpha)} w_{pq}(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b}). \tag{12}$$

The $\Pi_{a\alpha}$ operators can be considered as vectors

$$\mathbf{w}(a\alpha) = \left(w_{00}(a\alpha), w_{01}(a\alpha), \ldots, w_{mm}(a\alpha)\right), \quad m = d-1 \tag{13}$$

in the Hilbert space $\mathbb{C}^{d^2}$ of dimension d^2 endowed with the usual inner product

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta) = \sum_{p=0}^{d-1}\sum_{q=0}^{d-1} \overline{w_{pq}(a\alpha)} w_{pq}(b\beta) \tag{14}$$

(in Eq. (13), we use the dictionary order for ordering the components of $\mathbf{w}(a\alpha)$). Equation (12) can then be rewritten as

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1-\delta_{a,b}), \tag{15}$$

to be compared with Eq. (5).

The determination of the $\Pi_{a\alpha}$ operators and, therefore, of the $|a\alpha\rangle$ vectors in $\mathbb{C}^d$, is equivalent to the determination of the $w_{pq}(a\alpha)$ components of the $\mathbf{w}(a\alpha)$ vectors in $\mathbb{C}^{d^2}$. This yields the following.

Proposition 1. *For $d \geq 2$, to find $d+1$ MUBs in $\mathbb{C}^d$ (if they exist) is equivalent to find $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ in $\mathbb{C}^{d^2}$, of components $w_{pq}(a\alpha)$ such that $w_{pq}(a\alpha) = \overline{w_{qp}(a\alpha)}$ (with $p, q = 0, 1, \ldots, d-1$) and $\sum_{p=0}^{d-1} w_{pp}(a\alpha) = 1$, satisfying*

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(a\beta) = \delta_{\alpha,\beta} \tag{16}$$

and

$$\mathbf{w}(a\alpha)\cdot\mathbf{w}(b\beta) = \frac{1}{d} \text{ for } a \neq b, \tag{17}$$

where $a, b = 0, 1, \ldots, d$ and $\alpha = 0, 1, \ldots, d-1$.

Proof. The proof follows from Eqs. (6)–(15). □

For $a \neq b$, Eqs. (16) and (17) show that angle $\omega_{a\alpha b\beta}$ between any vector $\mathbf{w}(a\alpha)$ and any vector $\mathbf{w}(b\beta)$ is

$$\omega_{a\alpha b\beta} = \cos^{-1}(1/d) \tag{18}$$

and therefore does not depend on a, α, b and β.

Proposition 1 can be transcribed in terms of matrices. Let $M_{a\alpha}$ be the positive-semidefinite matrix of dimension d whose elements are $w_{pq}(a\alpha)$ with $p, q \in \mathbb{Z}/d\mathbb{Z}$. Then, Eq. (14) gives

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \mathrm{Tr}\left(M_{a\alpha} M_{b\beta}\right). \tag{19}$$

Therefore, we have the following proposition.

Proposition 2. *For $d \geq 2$, to find $d+1$ MUBs in $\mathbb{C}^d$ (if they exist) is equivalent to find $d(d+1)$ positive-semidefinite (and thus Hermitian) matrices $M_{a\alpha}$ of dimension d satisfying*

$$\mathrm{Tr}\left(M_{a\alpha}\right) = 1, \quad \mathrm{Tr}\left(M_{a\alpha} M_{b\beta}\right) = \delta_{\alpha,\beta}\delta_{a,b} + \frac{1}{d}(1 - \delta_{a,b}) \tag{20}$$

where $a, b = 0, 1, \ldots, d$ and $\alpha, \beta = 0, 1, \ldots, d-1$.

Proof. The proof is trivial. □

It is to be noted that Proposition 2 is in agreement with the result of Ref. [16] according to which a complete set of $d+1$ MUBs forms a convex polytope in the set of Hermitian matrices of dimension d and unit trace.

Finally, as a test of the validity of Propositions 1 and 2, we have the following result.

Proposition 3. *For d prime, Eqs. (16) and (17) or Eq. (20) admit the solution*

$$w_{pq}(a\alpha) = \frac{1}{d} \mathrm{e}^{\mathrm{i}\pi(p-q)[(d-2-p-q)a-2\alpha]/d}, \quad a, \alpha, p, q \in \mathbb{Z}/d\mathbb{Z} \tag{21}$$

and

$$w_{pq}(d\alpha) = \delta_{p,q}\delta_{p,\alpha}, \quad \alpha, p, q \in \mathbb{Z}/d\mathbb{Z} \tag{22}$$

for $a = d$.

Proof. The proof is based on the use of Gauss sums [17] in connection with ordinary [18] and quadratic [19] discrete Fourier transforms. Indeed, it is sufficient to calculate $\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta)$ as given by (14) with the help of (21) and (22) in the cases $a = b$ (for $a = 0, 1, \ldots, d$), $a \neq b$ (for $a, b = 0, 1, \ldots, d-1$) and $a \neq b$ (for $a = 0, 1, \ldots, d-1$ and $b = d$). The main steps are the following.

(i) Case $a = b = d$: We have

$$\mathbf{w}(d\alpha) \cdot \mathbf{w}(d\beta) = \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \delta_{p,q}\delta_{p,\alpha}\delta_{p,\beta} = \delta_{\alpha,\beta}. \tag{23}$$

(ii) Case $a = b = 0, 1, \ldots, d-1$: We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(a\beta) = \frac{1}{d^2} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{\mathrm{i}2\pi(p-q)(\alpha-\beta)/d} = \delta_{\alpha,\beta}. \tag{24}$$

(iii) Case $a \neq b$ ($a = 0, 1, \ldots, d-1$ and $b = d$): We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(d\beta) = \frac{1}{d} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{-\mathrm{i}\pi(p-q)[(d-2-p-q)a-2\alpha]/d} \delta_{p,q} \delta_{p,\alpha} = \frac{1}{d} \sum_{p=0}^{d-1} \delta_{p,\alpha} = \frac{1}{d}. \tag{25}$$

(iv) Case $a \neq b$ ($a, b = 0, 1, \ldots, d-1$): We have

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d^2} \sum_{p=0}^{d-1} \sum_{q=0}^{d-1} \mathrm{e}^{\mathrm{i}\pi(p-q)[(d-2-p-q)(b-a)+2(\alpha-\beta)]/d}. \tag{26}$$

The double sum in (26) can be factored into the product of two sums. This leads to

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d^2} \left| \sum_{k=0}^{d-1} \mathrm{e}^{\mathrm{i}\pi\{(a-b)k^2+[(d-2)(b-a)+2(\alpha-\beta)]k\}/d} \right|^2. \tag{27}$$

By introducing the generalized Gauss sums [17]

$$S(u, v, w) = \sum_{k=0}^{|w|-1} \mathrm{e}^{\mathrm{i}\pi(uk^2+vk)/w}, \tag{28}$$

(where u, v and w are integers such that u and w are coprime, uw is nonvanishing and $uw + v$ is even), we obtain

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d^2} |S(u, v, w)|^2, \tag{29}$$

with

$$u = a - b, \quad v = -(a-b)(d-2) + 2(\alpha - \beta), \quad w = d. \tag{30}$$

The $S(u, v, w)$ Gauss sum in (29)-(30) can be calculated from the methods in [17]. This yields

$$\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta) = \frac{1}{d}, \tag{31}$$

which completes the proof. □

4 Conclusion

As a conclusion, passing from $\mathbb{C}^d$ to $\mathbb{C}^{d^2}$ amounts to replace the square of the modulus of the inner product $\langle a\alpha | b\beta \rangle$ in $\mathbb{C}^d$ (see Eq. (5)) by the inner product $\mathbf{w}(a\alpha) \cdot \mathbf{w}(b\beta)$ in $\mathbb{C}^{d^2}$ (see Eqs. (16) and (17)). It is expected that the determination of the $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ satisfying Eqs. (16) and (17) (or the $d(d+1)$ corresponding matrices $M_{a\alpha}$ satisfying Eq. (20)) should be easier than the determination of the $d(d+1)$ vectors $|a\alpha\rangle$ satisfying Eq. (5). In this respect, the absence of a modulus in (17) represents an incremental step.

Now we may ask the question: How to pass from the $\mathbf{w}(a\alpha)$ to $|a\alpha\rangle$ vectors? Suppose we find $d(d+1)$ vectors of type (13) satisfying Eqs. (16) and (17). Then, the $\Pi_{a\alpha}$ operators given by

(8) are known. A matrix realization of each $\Pi_{a\alpha}$ operator immediately follows from the standard matrix realization of the generators of the $\mathrm{GL}(d,\mathbb{C})$ group. The eigenvector of the matrix of $\Pi_{a\alpha}$ corresponding to the eigenvalue equal to 1 gives the $|a\alpha\rangle$ vector.

Of course, the impossibility of finding $d(d+1)$ vectors $\mathbf{w}(a\alpha)$ or $d(d+1)$ matrices $M_{a\alpha}$ would mean that $d+1$ MUBs do not exist in $\mathbb{C}^d$ when d is not a strictly positive power of a prime.

Transforming a given problem into another one is always interesting even in the case where the new problem does not lead to the solution of the first one. In this vein, the existence problem of MUBs in d dimensions was approached from the points of view of finite geometry, Latin squares, and Hadamard matrices (see [6] and references therein) with some interesting developments. We hope that the results presented here will stimulate further works, especially a new way to handle the $d = 6$ unsolved problem.

To close, let us mention that it should be interesting to apply the developments in this paper to the concept of *weakly* MUBs recently introduced for dealing in the $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ phase space [20].

An extended version of this note will be published elsewhere.

References

[1] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, Z4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, Proc. London Math. Soc. **75**, 436 (1997).

[2] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Phys. Rev. Lett. **88**, 127902 (4 pages) (2002).

[3] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Discrete phase space based on finite fields, Phys. Rev. A **70**, 062101 (23 pages) (2004).

[4] B.-G. Englert and Y. Aharonov, The mean king's problem: prime degrees of freedom, Phys. Lett. A **284**, 1 (2001).

[5] J. Tolar, and G. Chadzitaskos, Feynman's path integral and mutually unbiased bases, J. Phys. A: Math. Theor. **42**, 245306 (11 pages) (2009).

[6] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, Internat. J. Quantum Info. **8**, 535 (2010).

[7] M. R. Kibler, An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, unitary group and Pauli group, J. Phys. A: Math. Theor. **42**, 353001 (28 pages) (2009).

[8] I. D. Ivanović, Geometrical description of quantum state determination, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[9] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. (N.Y.) **191**, 363 (1989).

[10] M. Grassl, Tomography of quantum states in small dimensions, Elec. Notes Discrete Math. **20**, 151 (2005).

[11] I. Bengtsson, W. Bruzda, Å. Ericsson, J. Å. Larsson, W. Tadej, and K. Życzkowski, Mutually unbiased bases and Hadamard matrices of order six, J. Math. Phys. **48**, 052106 (21 pages) (2007).

[12] S. Brierley and S. Weigert, Constructing mutually unbiased bases in dimension six, Phys. Rev. A **79**, 052316 (13 pages) (2009).

[13] D. McNulty and S. Weigert, The limited role of mutually unbiased product bases in dimension 6, J. Phys. A: Math. Theor. **45** 102001 (5 pages) (2012).

[14] D. McNulty and S. Weigert, On the impossibility to extend triples of mutually unbiased product bases in dimension six, arXiv:1203.6887.

[15] O. Albouy and M. R. Kibler, A unified approach to SIC-POVMs and MUBs, J. Russian Laser Res. **28**, 429 (2007).

[16] I. Bengtsson and Å. Ericsson, Mutually unbiased bases and the complementary polytope, Open Syst. Inf. Dyn. **12**, 107 (2005).

[17] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums* (New York: Wiley, 1998).

[18] A. Vourdas, Quantum systems with finite Hilbert space, Rep. Prog. Phys. **67**, 267 (2004).

[19] M. R. Kibler, "Quadratic discrete Fourier transform and mutually unbiased bases," in: *Fourier Transforms - Approach to Scientific Principles*, edited by G. Nikolic (Rijeka: In-Tech, 2011).

[20] M. Shalaby and A. Vourdas, Weak mutually unbiased bases, J. Phys. A: Math. Theor. **45**, 052001 (15 pages) (2012).